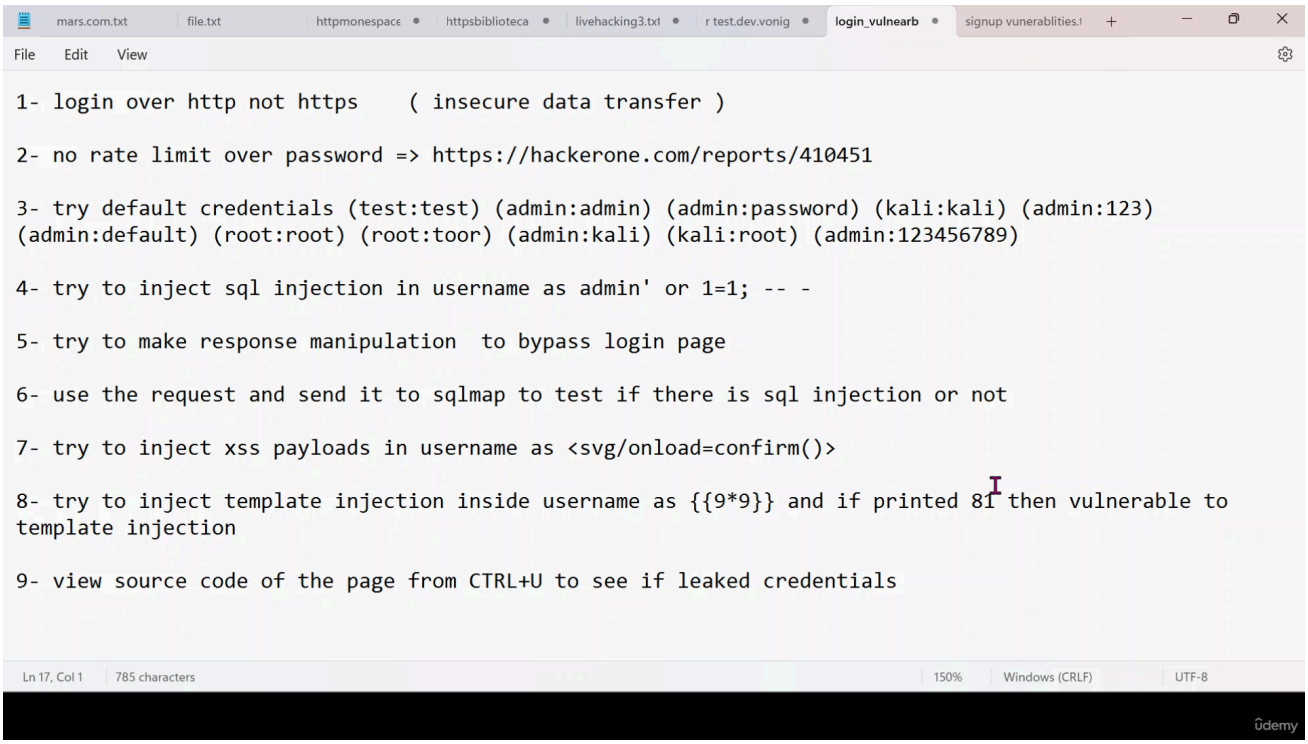
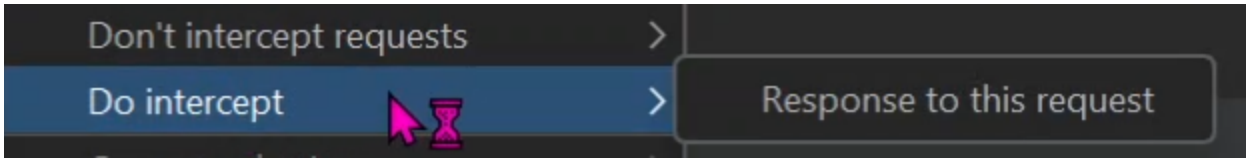
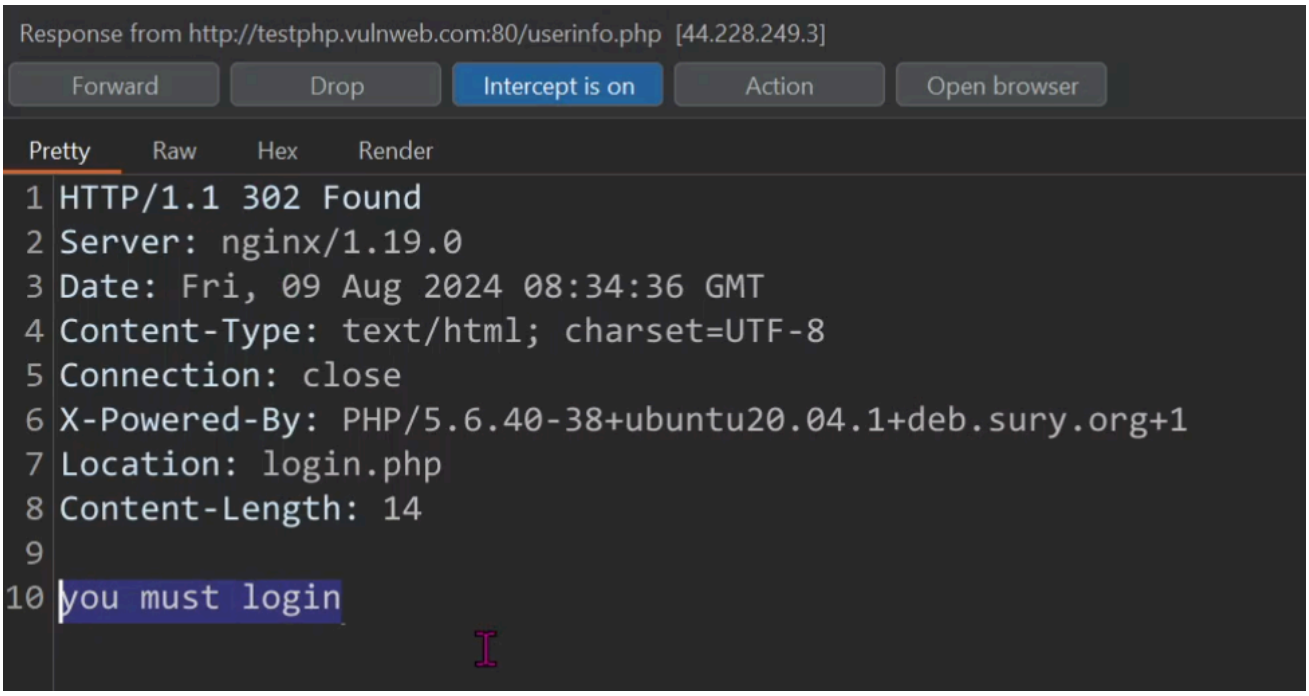
# Login Vulnerabilities Explain

- بتبقي موجوده ف صفحه الـ login

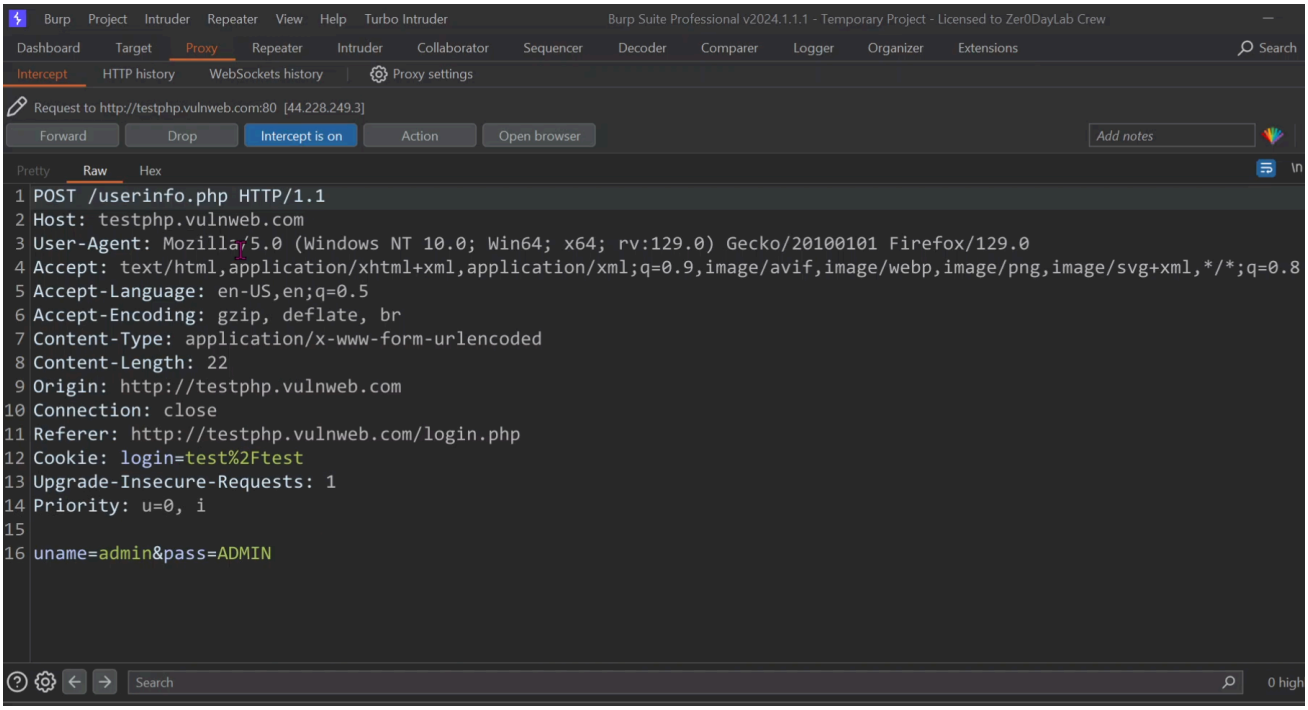



- 1 - لو لقيت صفحه ال login معموله Http تبقي not secure ممكن اي هاكر يعمل man in the middle attack ووقتها الباسورد بيبقي مش مؤمن بالقدر الكافي ودي ثغره اسمها ( insecure data transfer )
- 2 - بتجرب تكتب الـ user والـ pass غلط كذا مره شوف هيحظرك ولا لا لو في محاولات no rate limit
- 3 - بتجرب ال user وال pass ال default دول امثله بتجربهم
- 4 - بتحاول تعمل حقن فمكان الuser بتستخدم ثغره ال sql injection
- 5 - بتخش تعمل login بباسورد غلط وبتوقف الطلب ب burp بعد كدا بتعمل Do intercept وتختار Response to this request وتعمل forward للطلب






- بعدها بتحاول تغيرر ف الطلب لو جابلك False تغيرها ب True ولو جالك 0 تغيره ل 1 لو قالك failed تغيره ل successfull
- لو ف ال header جالك 403 forbidden بتغيره ل 200 OK
- 6 - بتستخدم ال sqlmap بس بتستخدمه ف ال request بتوقف الطلب وتاخد ال request كلو copy وتحطه ف ملف وتدخله علي ال sqlmap -r file.txt




- 7 - حاول تحقن xss payload ف ال username زي دا <()svg/onload=confirm>
- 8 - بتحاول تحط template injection زي دا {{9*9}} معناها انك بتحاول تنفذ اوامر تشوف هتتنفذ ولا لا
- 9 - بتعمل view page sourse لصفحه ال login وتحلل كود ال js تشوف فيه ثغره ولا لا

1- login over http not https ( insecure data transfer )

2- no rate limit over password => https://hackerone.com/reports/410451

3- try default credentials (test:test) (admin:admin) (admin:password) (kali:kali) (admin:123) (admin:default) (root:root) (root:toor) (admin:kali) (kali:root) (admin:123456789)

4- try to inject sql injection in username as admin' or 1=1; -- -

5- try to make response manipulation to bypass login page

6- use the request and send it to sqlmap to test if there is sql injection or not

7- try to inject xss payloads in username as <svg/onload=confirm()>

8- try to inject template injection inside username as {{9*9}} and if printed 81 then vulnerable to template injection

9- view source code of the page from CTRL+U to see if leaked credentials